Elektronische Zustellung LDAP Schemabeschreibung			**Konvention** **zuseldap-1.4.0** **Ergebnis der AG**
Kurzbeschreibung	Die elektronische Zustellung verwendet Verzeichnisdienste zur Informationsverteilung. Das vorliegende Dokument beschreibt das LDAP – Schema des Verzeichnisdienstes eines Zustelldienstes bzw. des Zustellkopfes.		
Autor(en):	Arne Tauber Peter Reichstädter	Projektteam / Arbeitsgruppe: AG-ZUSE / AG-II	
Beiträge von:	Bernhard Karning		

Version 1.4.0 : **02.02.2012**	Fristablauf: **TT.MM.JJJJ**
Abgelehnt von:	*(Länderangabe bei ablehnender Stellungnahme)*

Unter-Version ... : **TT.MM.JJJJ**	Fristablauf: **TT.MM.JJJJ**
Abgelehnt von:	*(Länderangabe bei ablehnender Stellungnahme)*

Detail-Version ... : **TT.MM.JJJJ**	Fristablauf: **TT.MM.JJJJ**
Anmerkungen:	*(Detailangaben zur Freigabe)*

Inhaltsverzeichnis

1. Einleitung

1.1. Abkürzungen

Tabelle 1 – Akronyme, die in dieser Spezifikation benutzt werden

Akronym	Erläuterung
DIT	Directory Information Tree
LDAP	Lightweight Directory Access Protocol
DN	Distinguished Name
bPK	Bereichsspezifisches Personenkennzeichen
ZMR	Zentrales Melderegister
ERnP	Ergänzungsregister für natürliche Personen

Die LDAP-spezifischen Abkürzungen sind entweder in den zugehörigen Standards definiert oder in den Schemadarstellungen erläutert.

1.2. Einleitung

Der Verzeichnisdienst des Zustelldienstes ist ein Service im Konzept der elektronischen Zustellung, der dem Zustellkopf via Push Protokoll [ZUSEPUSH] die erforderlichen Informationen über die Registrierung eines Empfängers im Rahmen der elektronischen Zustellung bzw. dessen Änderung der Stammdaten zur Verfügung stellt.

Die detaillierte Beschreibung des Zustellprozesses ist im Dokument Modell der elektronischen Zustellung [ZUSEMOD] enthalten. Die Prozessspezifikationen für die einzelnen Prozesse des Zustellverfahrens sind in den Dokumenten „Elektronische Zustellung – Technische Spezifikation“ [ZUSESPEC] bzw. „Elektronische Zustellung – Message Spezifikation“ [ZUSEMSG] definiert.

1.3. Verwendete Standards

Für die Spezifikation des LDAP-Modells für den Verzeichnisdienst des Zustelldienstes wird der Standard Lightweight Directory Access Protocol (v3) (LDAP v3) gemäß [RFC2251] zugrunde gelegt. Die Attributdefinition des vorliegenden Schemas bezieht sich auf den Standard Lightweight Directory Access Protocol (v3): Attribute Syntax Definition gemäß [RFC2252].

1.4. Verzeichnisdienst und Zustellung

Die elektronische Zustellung setzt voraus, dass jeder Zustelldienst einen Verzeichnisdienst betreibt, der den oben angeführten Standards entspricht und die Daten in einer dem nachstehend beschriebenen Schema entsprechenden Struktur bereithält bzw. unverzüglich gemäß [ZUSEPUSH] an den Zustellkopf übermittelt .

Ein zentraler Verzeichnisdienst (Zustellkopf) beantwortet die von den Versendern gestellten Anfragen durch Abfragen seines Verzeichnisses aller Empfängerinformationen. Der Zustellkopf selbst erhält sämtliche Empfängerinformationen von allen registrierten Zustelldiensten über das Push Protokoll [ZUSEPUSH]. Das Verzeichnis des Zustellkopfs ist somit eine Akkumulation der Verzeichnisdienste aller zugelassenen Zustelldienste.

2. LDAP Modell

2.1. Directory Information Tree

- Das DIT-Root Objekt (Klasse Objekt) hat den DN dc=at.
- Auf der zweiten Hierarchie-Ebene sind Container-Objekte der Klasse organization, die für jeden einzelnen Zustelldienst getrennte Namensräume schaffen. Dies ermöglicht eine einfache Verwaltung und Zugriffsmanagement für die einzelnen Zustelldienste. Die Vergabe der Organisationsbezeichnung an einen Zustelldienst erfolgt durch die den Zustellkopf betreibende Stelle im Zuge der Zulassung eines Zustelldienstes.
- Auf der dritten Hierarchieebene sind Container-Objekte der Klasse OrganizationalUnit, die getrennte Namensräume schaffen für natürliche und juristische Personen.

2.2. Klassen- und Attributbeschreibung

In der Spalte Eigenschaften eines Attributes bedeutet:

M bedeutet *mandatory* (= *required);* Default ist *optional (allowed).*

L bedeutet *multi-valued,* leer (Default) bedeutet *single-valued*

Typen:

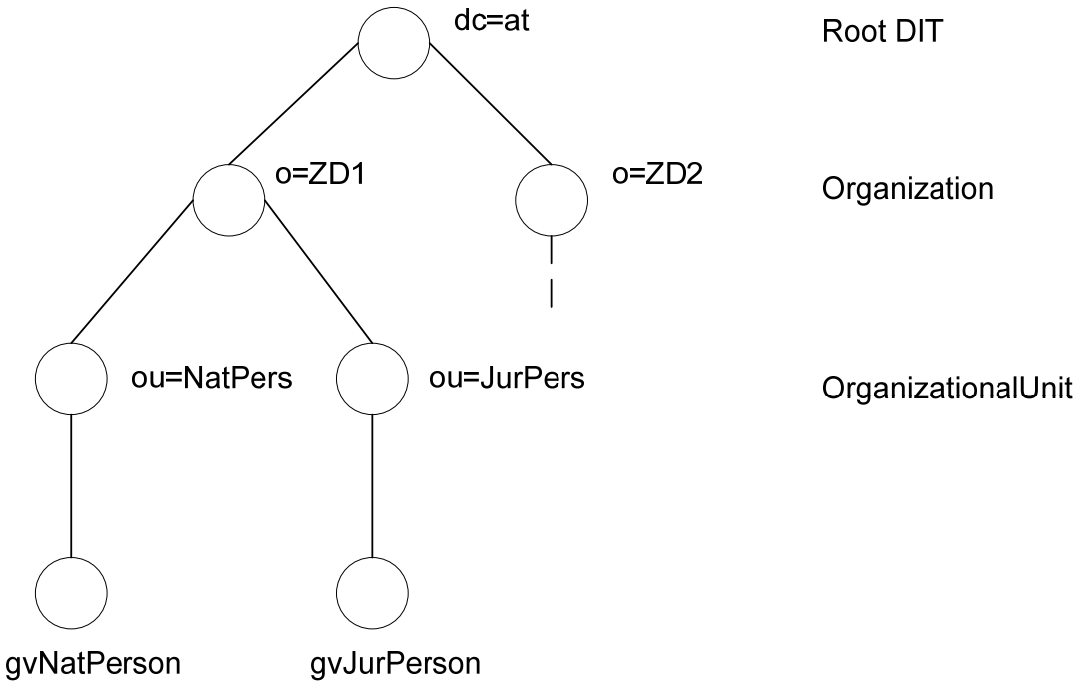
- **bin** binary
- **bool** Boolean Wert: TRUE oder FALSE
- **cis** Directory String, Case Insensitive Match (Default) Directory String, Case
- **ces** exact Match
- **date** Datum Format: JJJJ-MM-TT
- **dn** Distinguished Name
- **int** Integer
- **tel** Telephone Number: +LL VVVV AAAAAAA
- L: Landescode; V: Vorwahl; A: Nummer gemäß [ITU-TE123]
- **uri** URI [RFC2396]
- **mail** E-Mail Adresse gemäß [RFC2822]

Alle Attribute, die nicht in einem RFC definiert sind, haben den Präfix ‘gv’.

2.3. Verwendung der Klassen im DIT

Im folgenden Schema wird dargestellt, wie Objekte in Abhängigkeit von ihren Klassen im DIT (Directory Information Tree) positioniert werden:

Abbildung 1 – Klassen im DIT



- gvNatPerson: Natürliche Personen, identifiziert durch das Zustell-bPK. Namensschreibweise wie in der Personenbindung der Bürgerkarte enthalten.
- gvJurPerson: Juristische Personen, zum Beispiel:
  - registrierte Firmen (Firmenbuch)
  - Vereine (Vereinsregister)
  - Behörden (entsprechend der einschlägigen Gesetze)
  - Selbstverwaltungskörperschaften
  - Registrierte Genossenschaften
  - Nicht registrierte Einzelunternehmer
  - Andere nicht registrierte juristische Personen (z.B. GesmbR)
  - Ausländische juristische Personen
  - Betroffene, die im ERsB eingetragen sind
  - uva.
- Unterhalb der Namensräume, die durch die Knoten der Klasse organizationalUnit definiert sind, gibt es keine weitere hierarchische Untergliederung.

3. Objektklassen

3.1. Objektklasse gvNatPerson

Tabelle 2 – Attribute der Objektklasse gvNatPerson

gvNatPerson 1.2.40.0.10.2.1.0.100	Natürliche Person	
dn: gvZbPk *(dn: gvZbPk=E8XfYRKHDiky/QL5q7k/L9kgMfU=, ou=NatPers, o=ZD1, dc=at)*		
Attribut	**Beschreibung**	**Eigenschaft**
gvZbPK	Bereichsspezifisches Personenkennzeichen für den Bereich ZU (Zustellung), Base64 – kodiert *(E8XfYRKHDiky/QL5q7k/L9kgMfU=)*	ces,M
cn	(Doppel-)Vorname(n) Nachname *(Max Moritz Mustermann)*	cis,M
sn	Nachname laut Personenbindung *(Mustermann)*	cis,M
givenName	(Doppel-)Vorname(n) laut Personenbindung *(Max Moritz)*	cis,M
gvBirthdate	Geburtsdatum (laut Personenbindung) *(1979-08-21)*	date,M
street	Strasse und Hausnummer der Abgabestelle *(Ballhausplatz 2)*	Cis
l	Ort der Abgabestelle *(Wien)*	cis
c	Land der Abgabestelle (2-stelliges Kürzel nach ISO 3166-1) *(AT)*	cis
postalCode	PLZ der Abgabestelle *(1014)*	cis
mail	E-Mail-Adresse Format gemäß [RFC2822] *(max.moritz@mustermann.at)*	mail,M,L
telephoneNumber	Festnetz-, Fax- oder Mobiltelfonnummer Format gemäß [ITU-TE123] *(+43 1 5551234)*	tel,L
gvAcceptedFormat	MIME-Typ eines akzeptierten Dokumentformats	cis,M,L
gvAbsentFrom	keine Zustellung ab	date

gvAbsentUntil	keine Zustellung bis	date
gvAcceptPrivate	akzeptieren von privaten Zusendungen	bool,M
userCertificate	Zertifikat des Empfängers im X.509 Format, [DER] kodiert, welches den öffentlichen Schlüssel enthält	bin
gvCRRCheckBirthdate	ZMR Check auf Eindeutigkeit bezüglich VN + FN + Geb.Datum (siehe [ZUSEPUSH])	bool,M
gvCRRCheckAddress	ZMR Check auf Eindeutigkeit bezüglich VN + FN + Abgabestelle (siehe [ZUSEPUSH])	bool

3.2. Objektklasse gvJurPerson

Tabelle 3 – Attribute der Objektklasse gvJurPerson

gvJurPerson 1.2.40.0.10.2.1.0.101	Juristische Person	
dn: gvSourcePIN *(dn: gvSourcePIN=123456d, ou=JurPers, o=ZD1, dc=at)*		
Attribut	**Beschreibung**	**Eigenschaft**
gvSourcePIN	Stammzahl der juristischen Person *(123456d)*	ces, M
gvSourcePINType	Typangabe der juristischen Person, d.h. Angabe des Registers in dem diese Person geführt wird. Für Firmenbuch: urn:publicid:gv.at:baseid+XFN Für ZVR: urn:publicid:gv.at:baseid+XZVR Für ErsB: urn:publicid:gv.at:baseid+XERSB	ces, M
cn	Bezeichnung der juristischen Person	cis, M
sn	wie gvNatPerson, ***aber nicht mandatory***	
givenName	wie gvNatPerson, ***aber nicht mandatory***	
gvBirthdate	wie gvNatPerson, ***aber nicht mandatory***	
street	wie gvNatPerson	
l	wie gvNatPerson	
c	wie gvNatPerson	
postalCode	wie gvNatPerson	
mail	wie gvNatPerson	
telephoneNumber	wie gvNatPerson	
gvAcceptedFormat	wie gvNatPerson	
gvAbsentFrom	wie gvNatPerson	

gvAbsentUntil	wie gvNatPerson	
gvAcceptPrivate	wie gvNatPerson	
gvDirectoryInclude	Aufnahme in öffentliches Verzeichnis des Zustellkopfs	bool
gvMailBox	Sub-postfach des Empfängers	ces,L
gvERVCode	ERV-Code des Empfängers Für Teilnehmer des Elektronischen Rechtsverkehrs	ces
userCertificate	wie gvNatPerson	

Die juristische Person kann allerdings in bestimmten Fällen (z.B. bei einer Personengesellschaft) auch mit den Attributen einer natürlichen Person definiert werden und in diesen Fällen sind die dafür vorbereiteten Attribute zu verwenden. In allen anderen Fällen stellen sie aber kein Abfragekriterium dar und sind daher nicht als mandatory zu beschreiben.

4. Object Identifier der Attribute und Objektklassen

4.1. Objektklassen

Tabelle 4 – OIDs der Objektklasses gvNatPerson und gvJurPerson

Abk.	Name	Spezifikation	OID
	gvNatPerson	Ebenda	1.2.40.0.10.2.1.0.100
	gvJurPerson	Ebenda	1.2.40.0.10.2.1.0.101

4.2. Attribute

Tabelle 5 – OIDs der einzelnen Attribute

Abk.	Name	Spezifikation	OID
c	countryName	RFC 2256	2.5.4.6
cn	commonName	RFC 2256	2.5.4.3
	givenName	RFC 2256	2.5.4.42
	gvAbsentFrom	Ebenda	1.2.40.0.10.2.1.1.105
	gvAbsentUntil	Ebenda	1.2.40.0.10.2.1.1.106
	gvAcceptedFormat	Ebenda	1.2.40.0.10.2.1.1.111
	gvBirthdate	LDAP-gv.at	1.2.40.0.10.2.1.1.55
	gvSourcePIN	Ebenda	1.2.40.0.10.2.1.1.108
	gvSourcePINType	Ebenda	1.2.40.0.10.2.1.1.253
	gvZbPK	Ebenda	1.2.40.0.10.2.1.1.101
	gvAcceptPrivate	Ebenda	1.2.40.0.10.2.1.1.112
	gvDirectoryInclude	Ebenda	1.2.40.0.10.2.1.1.273
	gvMailBox	Ebenda	1.2.40.0.10.2.1.1.275
l	localityName	RFC 2256	2.5.4.7
	Mail	RFC 2798	0.9.2342.19200300.100.1.3
	postalCode	RFC 2256	2.5.4.17
	Street	RFC 2256	2.5.4.9
sn	Surname	RFC 2256	2.5.4.4
	telephoneNumber	RFC 2256	2.5.4.20
	userCertificate	RFC 2256	2.5.4.36
	gvCRRCheckBirthdate	Ebenda	1.2.40.0.10.2.1.1.257
	gvCRRCheckAddress	Ebenda	1.2.40.0.10.2.1.1.259
	gvERVCode	Ebenda	1.2.40.0.10.2.1.1.277

OIDs beginnend mit 1.2.40.0.10.2.1.1 sind in [LDAP] definiert.

A. Abbildungsverzeichnis

B. Tabellenverzeichnis

C. Revision History

Version	Datum	Autor(en)	
1.3.1	30.4.2008	Arne Tauber (EGIZ) Peter Reichstädter (BKA)	Initialversion
1.3.2	06.05.2010	Arne Tauber (EGIZ), Peter Reichstädter (BKA)	Editorielle Korrekturen sowie sprachliche Klarstellungen und Detaillierungen von Elementen: • *3 Objektklassen* • *4 Object Identifier der Attribute und Objektklassen* *3.1. detailliert Vorname -> (Doppel-)Vorname(n)* *gvCRRCheckBirthdate* und *gvCRRCheckAddress* hinzugefügt – um Eindeutigkeit eines registrierten users (ZMR-Basischeck) festzulegen 3.2. *gvSourcePINType* zur Unterscheidung der Stammzahlen juristischer Personen ergänzt 4.2. obige neuen bzw. ergänzten Attribute mit OIDs versehen
1.4.0	25.01.2012	Arne Tauber (EGIZ) Peter Reichstädter (BKA)	Editorielle Korrekturen gvIncludeDirectory Attribut Anpassung an ZUSE Version 1.4.0 ERV-Code

D. Referenzen

[DER]	ITU-T Recommendation X. 690 (1997), ISO/IEC 8825-1: 1998, Information Technology ASN. 1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)
[ITU-TE123]	ITU-T Recommendation E.123, Notation for national and international telephone numbers, e-mail addresses and web addresses, Februar 2001
[LDAP]	R. Hörbe, R. Wollendorfer: Spezifikation LDAP-gv.at, LDAP-gv.at 2.2.0, Dezember 2003, http://reference.e-government.gv.at/
[RFC2046]	Freed, N und Borenstein, N: RFC 2046: Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types. IETF Request for Comment, November 1996. http://www.ietf.org/rfc/rfc2046.txt
[RFC2251]	Wahl, Howes, Kille: RFC 2251: Lightweight Directory Access Protocol (v3), Dezember 1997, http://www.ietf.org/rfc/rfc2251 .txt
[RFC2252]	Wahl et al: RFC 2252: Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions, Dezember 1997 http://www.ietf.org/rfc/rfc2252.txt
[RFC2256]	M. Whal, RFC 2256: A Summary of the X.500(96) User Schema for use with LDAPv3, December 1997
[RFC2396]	Berners-Lee et al: RFC 2396: Uniform Resource Identifiers (URI): Generic Syntax, August 1998, http://www. ietf.org/rfc/rfc2396.txt
[RFC2822]	Resnick: RFC 2822: Internet Message Format, http://www.ietf.org/rfc/rfc2822.txt
[RFC2798]	M. Smith: RFC 2798: Definition of the inetOrgPerson LDAP Object Class, April 2000, http://www.ietf.org/rfc/rfc2798.txt
[RFC3647]	S. Chokhani: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003, http://www.ietf.org/rfc/rfc3647.txt
[ZUSEMOD]	P. Reichstädter, A. Tauber, T. Rössler, Modell und Prozesse der elektronischen Zustellung, 1.4.0
[ZUSESPEC]	A. Tauber, T. Rössler, P. Reichstädter, Elektronische Zustellung – Technische Spezifikation, 1.4.0

[ZUSEPUSH]	A.Tauber, Elektronische Zustellung – Push Protokoll, 1.4.0.
[ZUSEMSG]	A. Tauber, T. Rössler, P. Reichstädter, Elektronische Zustellung – Message Spezifikation, 1.4.0